

骗子大脑逆向工程

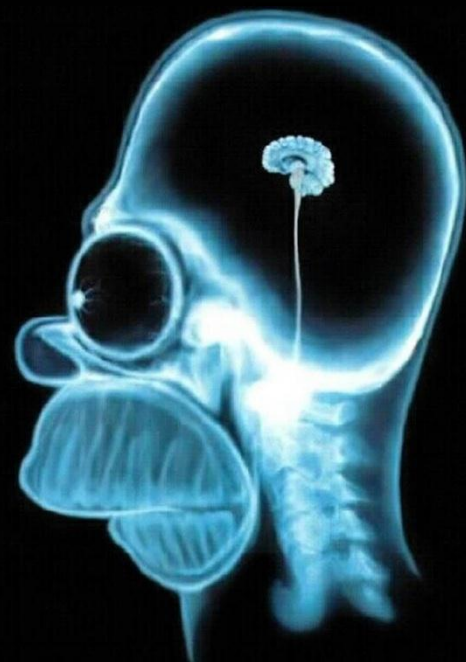
@neyolov evgeny

syscan360 | beijing



#我是？

- 网络犯罪分析
- 系统软件破解与取证
- 行业软件分析
- ZeroNights破解会议
- 俄国防御组织DCG#7812



#关于

- 投机公司项目
- 反被骗黑盒测试
- 诈骗技术的提升、行为分析



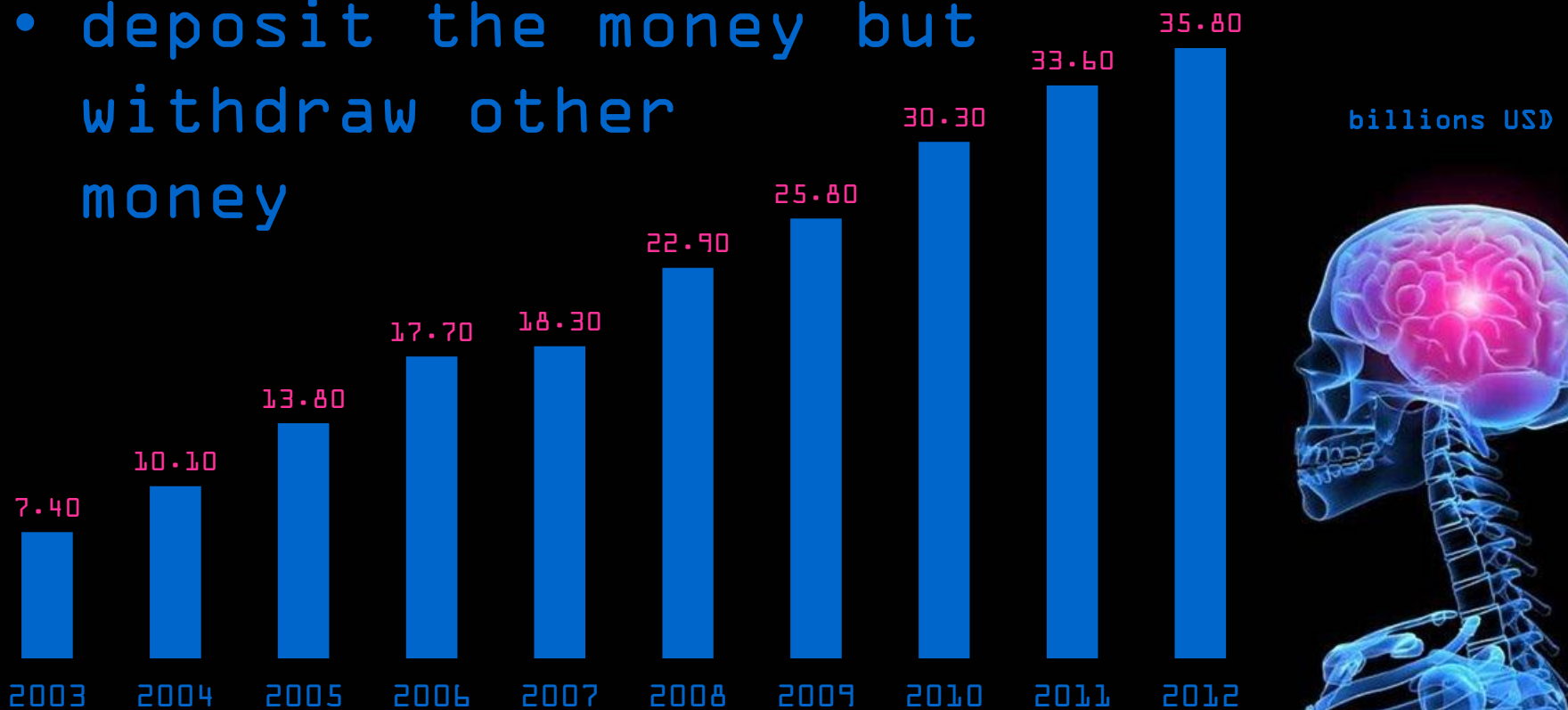
#投机

- 快速成长
- 巨大的市场
- 没有边界
- 永远生存



#利益

- 巨大市场成长
- 不可控金钱黑洞
- deposit the money but withdraw other money



问题

- 无视法律
- 无视数据保护
- 身份账户需求
- 近海位置
- 金融危机
- 洗钱
- 信用卡.



#例子

- 15 april 2011 - 黑色星期五
- 世界第二大扑克屋
- 像泡泡一样爆炸
- 充斥着欺骗
- 充斥的各种骗局的活动平台



不受惩戒

- 骗子非常自信不受惩戒
- 禁止最大惩戒
- 只是内部调查
- 申诉的经济限制
- 投机工业和法律盲点



#法律案件

- 大部分未知

例外：

- 奖金滥用坐牢 £80,000 ~ \$130,000
- 国际间不诚信
护照，身份证，
假支票



#范围

大部分：

- 扑克
- 赌场
- 打赌

小部分：

- 宾戈游戏
- 彩票
- 等等.



#攻略

- 玩家控制
- 反被骗检查

VS.

- 材料
- 平台
- 骗子培训
- 大众智慧



#顾客

- 身份
- 地址
- 经济信息
- 出生地和日期
- 邮箱和电话
- 个人住址



#顾客

- 身份
- 偷骗护照
- 地址
- Ip地址假支票
- 经济信息
- 假支票
- 出生地址和日期
- 偷骗护照
- 邮箱和电话
- 后台电话服务
- 个人住址
- 公寓假账户



#检查

- 操作系统帐号
- 浏览用户代理
- 系统注册
- 硬件帐号
- Mac地址
- Ip地址



#检查

- 操作系统帐号
 - 账户随机软件
- 浏览用户代理
 - 用户代理转换器
- 系统注册
 - 注册表清理
- 硬件帐号
 - 账户随机软件
- Mac地址
 - Mac变换
- IP地址
 - vpn, socks



#检查

- operating system IDs
 - ID randomization software
- browser user agent
 - user agent switchers
- system registry
 - registry cleaners
- hardware IDs
 - ID randomization software
- MAC address
 - MAC changers
- IP address
 - VPN, socks
- 一次插入=一台主机



#材料

虚拟机：

- 转换、随机化软件
- 反检测补丁



#材料

专用服务器：

- 给力主机
- 特定环境
- 企业数据中心私有服务器或者客户端系统
- 一次性使用



#活动

- 信用卡欺骗
- 账户接管
- 奖金劫持
- 附属程序翻烂
- 不公正操作



#卡

- 身份窃取
- 偷取信用卡信息
- 偷取持有者信息
- 2个剧本



#信用卡剧本1

全设置的绕过检测：

- 信用卡数据
- 个人帐号的硬件扫描检测
- 依赖上述的信息复制



FULLZ CC:	Fullz info:	Address 1:	Name On Card:
	Address 2:		Credit Card Number:
Name and surname:	City:		Credit Card Brand:
billing adress:	State:		Credit Card Type:
Address 1:	Zip:		Start Date:
Address 2:	Country:		EXP Date:
City:	Home Phone:		issue Number:
State:	Date Of Birth:		Credit Card PIN Number:
Zip:	Social Security Number:		Card ID Number:
Country:	Mothers Maiden Name:		Card Bank Name:
Home Phone:	Drivers License Number:		Card 1800 Number:
Name On Card:	Drivers License State:		email:
Credit Card Number:	Secret Question 1:		email pass:
Credit Card Type:	Secret Question Answer 1:		bank name:
EXP Date:	Secret Question 2:		Bank Account Number :
email:	Secret Question Answer2:		Bank Routing Number :
			bank phone:

#信用卡剧本2

幸运欺骗着游戏：

- 消费痕迹跟踪
- 自动修整产生假的个人账户
- 社会工程能力



#信用卡剧本2

- 需要pan和持有者名字.
- 这就够了么?
- ismycreditcardstolen.com
- twitter.com/needadebitcard



Debit Card

@NeedADebitCard

Please quit posting pictures of you



Niko S @nicknikoo

Debit card Chelsea Stamford Bridge pic.twitter.com/njkjD3QK

Retweeted by Debit Card

Hide photo Reply Retweet Favorite

26 Nov



3
RETWEETS

1
FAVORITE



6:41 AM - 26 Nov 12 - Details

Flag media

Reply to @nicknikoo



Major Hayden @rackerhacker

@nicknikoo Thanks for sharing. Can I buy something on your card?

Expand

26 Nov

Twe



Tweet to Debit Card

@NeedADebitCard

Tweets

Following

Followers

Favorites

Lists

Recent images



Similar to Debit Card



Gerd Eist @erdgeist

Follow

账户接管

- 谁的责任?
 - 投机操作者.
-
- 弱密钥恢复确认
 - 服务端脆弱点
 - 客户端的脆弱点
 - 数据破坏



账户接管

- 谁的责任?
 - 玩家.
-
- 敏感个人信息泄露
 - 恶意代码、木马、钓鱼



#账户接管

- 偷取所有账户资金
- 账户未设保护便可完全接管
- 用此账户来作为骗钱的入口点
- 贩卖账户在地下市场
- 肆意花这笔钱



#福利获取

- 延期服务
- 不损害合法玩家用户
- 不偷玩家资金
- 不盗取玩家帐号



#福利获取

- 附属程序滥用
- 福利提供者过多
- 套利打赌
- 其他不公平活动，像诈骗、芯片复制



附属程序滥用

- 注册附属账户
- 玩家????
- 利润!!!1



附属程序滥用

- 投机者有程序获得新的玩家账户
- 程序来自专业公司打造
- 公司不断查找新的附属合作者
- 骗子总是为了钱



#福利提供者泛滥

- 欢迎
- 重载
- 无保证金
- 难对付
- moneyback



#套利赌注

- 俩账户
- 俩产出
- 俩赌方
- 一个赢
- 保证玩家赢
- 保证操作者输



#ctf

- 抓住骗子
- 计划不同但是内部过程相似
- 一个账户多个骗点
- 四处寻找有趣的事情



#ctf

- c2c 地下市场
- 给力服务器的随机账户
- 真的一个账户一个消费者？
- 偷东西的过程中可曾新村神圣？





#案例1

- 安全事件日志， 登陆登出
- 事件ID 4624 (7) or 528 (XP)
- 登陆类型e 10 (via RDP)

- 服务用户名
- 域名
- 登录类型
- 客户端主机名
- IP地址





- События страницы сводки
- Журналы Windows
 - Приложение
 - Безопасность
 - Установка
 - Система
 - Перенаправленные события
- Журналы приложений и служб
 - Internet Explorer
 - Key Management Service
 - Media Center
 - Microsoft
 - Windows
 - API-Tracing
 - AppID
 - Application-Experience
 - AppLocker
 - Audio
 - Authentication User Interf...
 - Backup
 - Biometrics
 - Bits-Client
 - Bluetooth-MTPEnum
 - BranchCache
 - BranchCacheSMB
 - CAPI2
 - CertificateServicesClient-C
 - CertPolEng
 - CodeIntegrity
 - CorruptedFileRecovery-Cli
 - CorruptedFileRecovery-Se
 - DateTimeControlPanel

Свойства событий - Событие 4624, Microsoft Windows security auditing.

Общие Подробности

☒ Понятное представление ☐ Режим XML

TargetUserSid S-1-5-21-38503254-1057719598-1857940269-1000

TargetUserName [REDACTED]

TargetDomainName [REDACTED]

TargetLogonId 0x95cc43e

LogonType 10

LogonProcessName User32

AuthenticationPackageName Negotiate

WorkstationName [REDACTED]

LogonGuid {00000000-0000-

TransmittedServices -

LmPackageName -

KeyLength 0

ProcessId 0x17f8

ProcessName C:\Windows\System

IpAddress [REDACTED]

IpPort 1192

Копировать

Код события

4672
4624
4624
4648
4624
4672
4672
4634
4634
4624
4624
4634

WWW.IP-SCORE.COM
if we see, then others see..

Enter IP for check

IP information:

[REDACTED] Russian Federation

State: Moscow City

City: Moscow

ZIP: N/A

Hostname: [REDACTED] [Whois](#)

Organization: VL-Telecom Ltd

ISP: VL-Telecom Ltd

• IP address

案例1

应用程序和服务日志- 微软windows树
终端服务*：

- 远程桌面客户端
- 即插即用设备
- 客户端usb设备
- 本地会话管理
- 远程连接管理



案例2

- 开始菜单栏? are you kidding me?

- 假目标
- 硬件ID随机器
- 即时消息



Cavalliere 

 27.01.2012, 02:45

nikobellic

jid: nikobellic@exploit.im

icq: 174314 и 174-314

И так ситуация конечно трудная но она есть

► Продажа покер акков

nikobellic 

 5.10.2009, 21:48

WANTED
DANGER WITH A DEADLY WEAPON



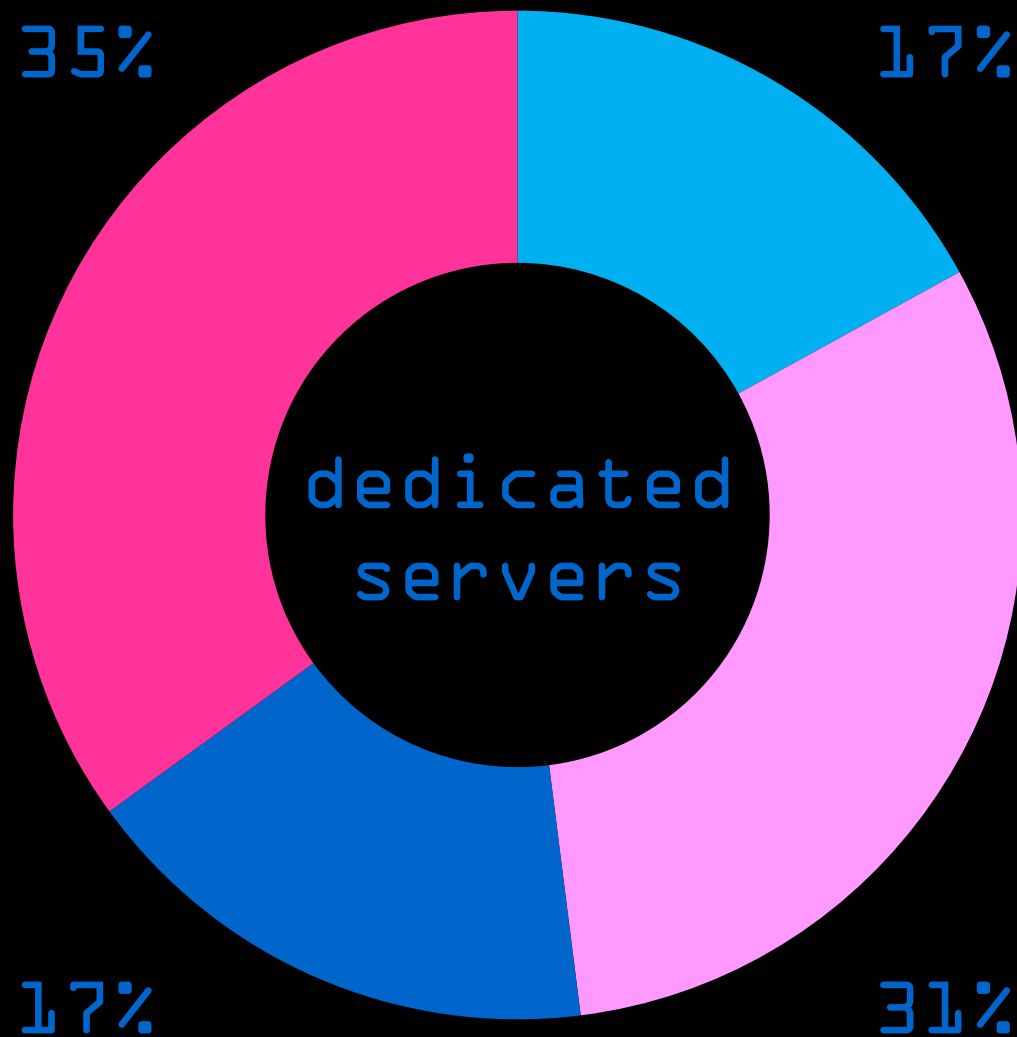
Продаю акки покера ,фултилт балансы от 500
цена за 500\$- 40wmz, + дедик в комплекте



DOUBLE FACEPALM

When the Fail is so strong, one Facepalm is not enough.

证据



#智慧总结

it seems his favorite phrase

天网恢恢疏而不
亲爱的骗子，
你能更高明点，
给我点儿挑战



#推荐阅读

- global gaming outlook <http://goo.gl/PntLS>
- a gamble or a sure bet? <http://goo.gl/n8YYZ>
- gambling knowledgebase <http://goo.gl/wmvsc>
- jailed for bonus abuse <http://goo.gl/vttJ7>
- AML and CTF <http://goo.gl/lWqUi>



#you are welcome ^_^

twitter.com/neyolov

neyolov@erpscan.com

